



POINTS OF INTEREST

- Employee Recognition
- Under Age/
Under Arrest
- Flag Day
- Birthdays
- Retirement
- Promotions/New Hires
- Department News
- Recipes

Good Spirits

JUNE 2014

Stores Division Employee Recognition



Karla Morse—Manager Store #84

On Tuesday, May 13 at the monthly ABC Board Meeting the Sales Manager and Sales Associate of the Year were recognized along with all of the nominees. After the meeting all the nominees were treated to Cake and Punch in the Enforcement Training room. There were four (4) Sales Managers and six (6) Sales

Associates nominated. The 2013 Sales Manger of the year was Karla Morse, Manager Store #84 - Mobile and the 2013 Sales Associate of the year was Russell Blake Smitherman, Store #102—Tuscaloosa. The nominees were Sales Manager—Blair Morgan Garmon, Store #104—Pell City, Renita Tucker, Store #134 - Brent, and Alonzo Williams, Store #136—Tuscaloosa.



Russell B. Smitherman, SA—Store #102



The 2013 Winners and the Nominees

The 2013 Sales Associates nominees were Santana Houghton, Store #3—Montgomery, Jerrel McDaniel Jr., Store #99 –Dadeville, Steve Crosby, Store #108—Dothan, Starr Anglin, Store #119 –Ozark and Jonathan Blake Wilford, Store #125—Pelham.

We would like to congratulate the winners and the nominees. Thanks for the job that you do it is greatly appreciated.

2013 Sales Manager of the Year Nominees



Blair Morgan Garmon, Manager
104—Pell City



Alonzo Williams, Manager
136—Tuscaloosa



Renita Tucker, Manager 134—
Brent



2013 Sales Associate of the Year Nominees



Jerrold McDaniel Jr. Store 99—
Dadeville



Santina Houghton, Store 003—
Montgomery



Steve Cosby, Store #108 -
Dothan



Starr Anglin, Store 119—Ozark



Blake Wilford, Store 125—
Pelham



Under Age—Under Arrest - Mac Gipson, Administrator speaks at Gadsden City High School!

Messenger

book.com/themessengergadsden

Community Paper

May 2, 2014

www.gadsdenmessenger.com • 50

Learning the cost of drunk driving

By Donna Thornton
News Editor.

Upperclassmen at Gadsden City High School learned the harsh reality drinking under the age of 21 last week, when the Alabama Beverage Control Board brought its "Under Age, Under Arrest" program to the school.

But the lessons about the legal risks they face from underage drinking may not be the most lasting lessons.

The students also heard from Renza Avery of the Gadsden Police Department.

Avery is now a resource officer at the school, but in 1993, he almost became a statistic — another victim of a drunk driver.

Avery was seriously injured in car crash when a drunk 16-year-old driver pulled out in front of his patrol car.

The driver and his brother both died in the crash.

His words regarding drinking and driving were simple: "Just don't do it. It affects not only you, but everyone around you."

The program came prior to Gadsden's prom, in an effort to persuade students to make safe choices on prom night and beyond. Students were supplied with pledge cards and asked to sign and submit them after the program.

In addition to hearing from Avery, Joyce Jones told the story of what happened to her son, Marcus Mitchell, another victim of a drunk driver.

Marcus was a promising student and basketball player.

He'd just completed his freshman year at Tuskegee and his coach wanted him to be a captain in the coming season.

He had come home from Tuskegee, dropping off a friend at his house. He and

other friends went to Birmingham and were driving home in the rain. Marcus fell asleep in the car, as

"I wouldn't want any of your parents to feel the way I felt, the way I still feel today," Jones said, over the loss of her son.

one of his friends drove.

"Someone had called to report to the sheriff's department that someone was driving on the wrong side of the road," Jones said.

"The sheriff's department didn't get there in time."

Her family received the call in the night and rushed to Carraway Hospital. Her son had been gravely injured.

Friends and family arrived, Jones told a very quiet auditorium of teenagers.

"They fill you with the false hope," Jones said, and getting Marcus better, taking him home and sending him back to college.

Then a nurse came, asking if they wanted to donate his organs.

"I said 'Why would we want to do that?'"

Then doctors took her and Marcus' father to another room and said, "We're sorry, he's not going to make it."

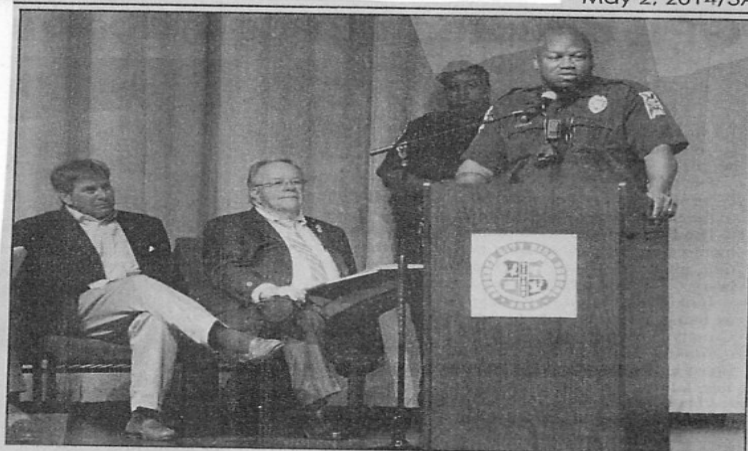
When the nurse came back to them, they agreed to donate his organs.

"The one thing we couldn't give away was his eyes, his corneas," Jones said.

"I told them I wanted him to play basketball with the angels and he needed his eyes to see."

"I wouldn't want any of your parents to feel the way I felt, the way I still feel today," Jones said, over the loss of her son.

"Even if you're not drinking and driving, if you know someone who's drinking and driving, you tell them a little about me ... coming here, baring my soul to you because a drunk driver made the wrong decision," Jones told the students.



May 2, 2014/3A

Donna Thornton/Messenger

Alabama House Minority Leader Craig Ford, Alabama Alcoholic Beverage Control Board Administrator Mac Gipson and Gadsden City High School Resource Officer Sylvia Slick listen as GCHS SRO Renza Avery describes a car crash that could have claimed his life. The intoxicated teen driving the other vehicle and his brother died in the crash.

Flag Day - June 14

Flag Day is observed in the United States on June 14. It commemorates the day in 1777 when the Continental Congress adopted the Stars and Stripes as our flag. It then had only 13 stars, to match its 13 stripes.

It's not an official national holiday, but in Pennsylvania, it is a legal holiday. The President has proclaimed a public flag day observance every year. It was first observed to celebrate the 100th anniversary of the selection of the flag.

President Harry S. Truman officially recognized June 14 as Flag Day by signing the National Flag Day Bill.



July 2

Dee McCain, Store #14
Kenny Osborne, Accounting
Susie Yarbrough, Stores
Robert Hill, Attorney
Kynatter Bell, Store #56

July 4

Jim Cascio, Store #83
John Richardson, Enforcement
Scott Bagby, Store #67

July 6

Lee Lawrence, Enforcement
Gail Bolar, Store #67

July 7

Jonathan Graham, Enforcement
Cedric Burton, Warehouse

July 7

Jonathan Graham, Enforcement
Cedric Burton, Warehouse

July 8

Ray Nicholson, Store #8
Anne Smitherman, Accounting
Amy Paillette, Enforcement
Mary Adkins, Enforcement
Janice Tibbets, Enforcement
Keven Kolego, Store #132
Ashlie Marshall, Store #100

July 10

Melissa Marshall, Store #136

July 11

Stephen Tidwell, Enforcement

July 12

Don Pettaway, Store #196
Randall Smith, Product Management
Katrina Garnett, Audit Division

July 13

Chad Allen, Enforcement

July 14

Denis Palmer, Store #84
Betty Dean, Enforcement
Sherrie Baty, Store #128

July 15

Kerri Barnett, Store #74

July 16

Brandon Blanton, Enforcement

July 17

Gene Schrieber, Enforcement

Michael Nolin, Store #34

Charlene Barnes, Store #165

July 18

Hazel J. Gilmore, Store # 164

Kelli Folmar, Audit Division

July 20

Demetrius Bogan, Enforcement

Starr Anglin, Floater D#7

Linda Goggins, Store #35

July 21

Faye Hand, Store #101

Chris Ransom, Store #97

July 22

Jerre Peak, Store #22

July 23

Carlton McClain, Store #53

Brittney Roberts, Enforcement

Latrenda McCain-Lee, Store #1

Bridgette Chamblee, Store #148



July 25

Christie Kramer, Store #79

July 27

Sandy Morris, Store #48

Kyle Odom, Store #126

Freddie Hubbard, Store #96

July 28

Linda Hubbard, Store #134

Russell Saunders, Store #123

July 29

RoBerta Chase, Store #42

David Waller, Store #73

Robert Frazier, Store #78

Kelly Roberts,. Store #9

July 31

Bob Martin, Attorney

Theresa McCool Store #102



Happy Belated Birthday!

May 5

Dean Argo, Government Relations Manager

June 3

Chameka Darrington, Sales Associate Store
#85

Congratulations on your Retirement!

H. Doug Atchison, Stores Division Store #114

James Posey, Warehouse

Charles Wall, Store #185

Sarah Lynaum, Store #84

Trish Montgomery, Supervisor D#12



Congratulations to

**John Rogers, Information Technology who
will be retiring July 1,**

SAY HELLO TO OUR

**NEW
HiRES**

FROM THIS MONTH!

Welcome to the ABC Board!

Dana Green, Sales Associate, Store #176

Braxton Vickery, Sales Associate, Store #176

Brandon Wright, Sales Associate, Store #125

James Nichols, Sales Associate, Store #125

**Chameka Darrington, Sales Associate Store
#85**

**JOB
CAREER
PROMOTION**

Congratulations on your Promotion:

Donna Speights, Manager III—Store #11

Greg Atchley, Manager I—Store #66

Cindy Byrd, Manager II—Store #150

**Jonathon Mahlke, IT Systems Technician Service,
Information Technology**



**I have to apologize to Store #164—
Mobile. I put the wrong store
number and city on this Easter
Display in the May Newsletter. This
wonderful display credit goes to Store
#164—Mobile—Hazel Gilmore,
Manager and Jackie Chapman, Sales
Associate.**

These Ladies did a great job!

**Store #75—Jackson decorated their store
for Memorial Day.**

Good Job—Hope, Mendy and Jackie!



The background of the entire page is a stylized American flag. The stars are a light blue color, and the stripes are a light red color. The flag is draped and folded, creating a sense of movement.

Store Division

PAGE 11

Congratulations to LaToya Howard, from Store #192 on Graduating from Jefferson State with a degree in Networking.

Congratulations LaToya!

Congratulations to Darrian Julks, the grandson of Sharon Julks, Manager Store #17 on his joint admissions to Lawson Community College and UAB. He will be majoring in Broadcasting and Journalism Technology.

Congratulations Darrian!

Congratulations to Robert Frazier and Natasha Jones on their recent promotions to Manager I.

Robert will be managing the new Wedowee Store #78 and Natasha will be the Manager I at Store #31 in Auburn

Congratulations Robert and Natasha!

Jordan Richardson, son of Genevieve Richardson, Manager at Store #102 Tuscaloosa, graduated with honors from Greene Co. High School in Eutaw May 29th 2014, he will be attending Shelton State his freshman year of college and then will be transferring to A & M University where he will be earning a degree in Engineering.

Congratulations Jordan!

Congratulations to Catharine Richardson, Manager II at Store #58 on June 6th is her 25th year with the state of Alabama.

Congratulations Catharine!

Store Division



Five Generations:

**Great-Great Grandmother,
Barbara Sims Hood**

**Great-Grandmother,
Susan Hood (Assistant Director)**

Rick Rubrigi, Grandfather

Rikki Lauren Rubrigi, Mother

Jace Alexander Usry, Born 3/7/14



Kaylee Downing the daughter of Mike Downing manager of Store #054 in Marion received the Most Valuable Player award for varsity volleyball at The Marion Academy annual sports banquet on May 16, 2014. Kaylee also received the award for most hustle in girls varsity basketball. She is shown here receiving the MVP award from athletic director and coach Scott Brewer.

Kaylee graduated from Marion Academy on Ma 23 and received The Fred Hubbard Memorial Scholarship. Kaylee will start her college career in the fall at Shelton State Junior College in Tuscaloosa.

Sorry to have to report that we lost a co-worker on Sunday, May 25. Tony Maddaox, Manager at Store #29. Please remember the Maddox family in your thoughts and prayers.

Also remember Debra Larison, Stores Director and her family. Ms. Larison Brother, Bill Simmons, past away on May 25. Please keep this family in your thoughts and prayers.

Product Management

PAGE 13



Congratulations to Catherine Sistrunk, Product Management on the marriage of her daughter. Courtney and Cedric where married on April 19, 2014

**Congratulations
Mr. & Mrs. Scott**

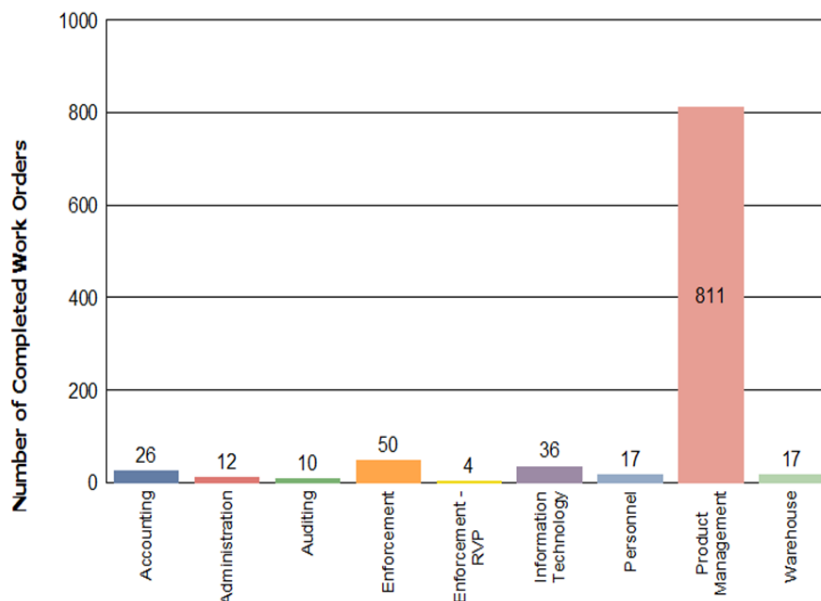
Information Technology

Completed Work Orders by Department

Dates displayed in
Central Daylight Time

From 4/1/2014
To 4/30/2014

5/16/2014 9:10:52AM



State of Alabama – Policies and Standards

POLICY 630-02: SYSTEM USE

Inappropriate use of State information technology (IT) resources exposes the State and its data to risks including potential virus attacks, compromise of network systems and services, and legal liabilities. Effective security is a team effort involving the participation and support of every employee and affiliate who deals with information and/or information systems. It is the responsibility of every IT user to know these rules and to conduct their activities accordingly. These rules are in place to protect the employee, the State, and the State's data.

OBJECTIVE:

Define acceptable and non-acceptable use of State-owned IT resources including systems and devices, software, Internet, and communications capabilities including e-mail, instant messaging, and social media.

SCOPE:

This policy applies to all Executive Branch agencies, boards, and commissions except those exempt under The Code of Alabama 1975 (Title 41 Chapter 4 Article 11).

SYSTEM USE POLICIES

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, and network accounts providing electronic mail, Internet access, and Web browsing are the property of the State of Alabama. These systems are to be used for business purposes in serving the interests of the government and of the people it serves in the course of normal operations.

PERSONAL USE:

Limited personal use of State-managed computing resources is anticipated; however, employees and managers are responsible for exercising good judgment regarding the reasonableness of personal use. Agencies may create additional policies concerning personal use of State information systems, but no agency policy may impose a lesser limitation on personal use than is prescribed by this policy.

PROHIBITED ACTIVITIES:

- ☐ The following activities are prohibited when using State IT resources:
 - ☐ Any activity that is illegal under local, state, federal or international law
 - ☐ Non-incidental personal use of State-managed computing resources
 - ☐ Activities in support of personal or private business enterprises
 - ☐ Unauthorized reproduction of copyrighted material
- ☐ Violating the rights of any person or other legal entity protected by copyright, trade secret, patent or other intellectual property laws, or similar laws or regulations, including, but not limited to, laws which protect against the installation or distribution of software products that are not appropriately licensed for use by the State
 - ☐ Exporting software, technical information, encryption software, or technology, in violation of international or regional export control laws
- ☐ Introducing malicious software (malware) into the network or systems (e.g., viruses, worms,
 - ☐ Trojan horses, logic bombs, etc.) within reason of user's control
 - ☐ Making fraudulent offers of products or services
- ☐ Making statements of warranty, expressed or implied, unless part of normal duties
- ☐ Accessing, possessing, or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction
- ☐ Accessing, possessing, or transmitting any sexually explicit, offensive, or inappropriate images and/or text
- ☐ Effecting security breaches or disruptions of network communication (security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless within the scope of regular duties; potential disruptions include, but are not limited to, port/IP scanning, packet sniffing, or IP spoofing)

State of Alabama – Policies and Standards

- ☐ Conducting network, system, or application scanning without IT Manager prior approval
- ☐ Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty
 - ☐ Circumventing user authentication or security of any host, network, or account
 - ☐ Interfering with or denying service to any user except in the course of assigned duties
- ☐ Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the network
- ☐ Accessing web sites offering online gambling, games, and related information such as cheats, codes, demos, online contests, role-playing games, traditional board games, game reviews, and sites that promote game manufacturers

EXCEPTIONS:

Employees may be exempted from some of these restrictions in the course of their legitimate job responsibilities (e.g., Investigative personnel may require access to web sites that are otherwise restricted).

IT Managers or Agency Heads shall request exceptions from the appropriate authority (e.g., Network Support, State IT Security Council, or Director, Information Services Division, Department of Finance).

INTERNET ACCESS POLICIES

Access to the Internet is provided as a business and informational resource to support and enhance the capability of Internet users to carry out their job responsibilities. Internet users are expected to handle their access privileges in a responsible manner and to follow all Internet-related policies and procedures. The State reserves the right to access, monitor, or disclose all Internet activity as required in the course of monitoring, auditing, or responding to legal processes or investigative procedures.

Users do not enjoy any right of personal privacy when using State-provided Internet services.

. All records

created as a result of using Internet services are government records. As such, these records are subject

to the provisions of state laws regarding their maintenance, access, and disposition.

Internet usage records may be public records under the Alabama public records laws and may be made

available to the public upon lawful request. If an agency deems their use of Internet services is an exception to the public records laws, the Agency Head shall request exception through the State

Records
Commission.

It is the responsibility of the Agency Head or Agency IT Manager to:

Ensure that each employee, agent, contractor, or other person utilizing Internet services has been advised of and understands all policies and restrictions applicable to the use of such services.

Take appropriate managerial and/or disciplinary action for inappropriate uses of Internet services by state employees or other persons accessing Internet services through that agency.

INTERNET CONTENT MANAGEMENT:

Use of State IT resources for the purpose of viewing, executing, or downloading content inappropriate for

official State business exposes the State and its data to risks including virus attacks, spyware and other

malware threats, compromise of network systems and services, and potential legal and liability issues.

State of Alabama – Policies and Standards

To mitigate these risks, access to certain categories of Internet content is restricted (blocked). By the authority of the Director, Information Services Division, Department of Finance, the following categories of Internet content present a threat to the security of State systems or have been deemed not

necessary for conducting official State business and are therefore blocked:

- ☐ Games and Gambling
- ☐ Malicious Websites
- ☐ Nudity and Risqué
- ☐ Phishing
- ☐ Peer-to-Peer File Sharing
- ☐ Pornography
- ☐ Proxy Avoidance
- ☐ Spam URLs

Any additional website(s) or category of sites not listed above may also be blocked if deemed a cyber security risk.

Exceptions may be granted to access blocked web sites for individuals or agencies that have a business need for access in order to do their jobs. Each request for access to a blocked web site requires a legitimate business need and written approval of the agency head or IT Manager and the Director, Information Services Division, Department of Finance.

E-MAIL USAGE POLICIES

To ensure the integrity and availability of e-mail system resources all electronic communications are expected to comply with relevant Federal and State laws as well as State policies and standards. The following requirements apply to the use of State-provided e-mail systems. E-mail shall be distributed, stored, and disposed of based on the data content in accordance with State information management requirements. E-mail content created, stored, transmitted, or received using State resources are the property of the State. Nothing in this policy shall be construed to waive any claim of privilege or confidentiality of email content. Authorized State personnel may access, monitor, or disclose e-mail content for state business purposes or to satisfy legal obligations.

PERSONAL USE OF STATE E-MAIL:

State e-mail systems are to be used for business purposes in serving the interests of the government and of the people it serves; however, incidental, occasional personal use of State e-mail is permitted. Employees and managers are responsible for exercising good judgment regarding the reasonableness

(frequency and duration) of personal use.

In accordance with The Code of Alabama, Section 36-25-5, state e-mail shall not be used for "personal gain."

State of Alabama – Policies and Standards

Personal e-mail shall be deleted or saved separately from work-related e-mail.

Users are permitted to include personal appointments in their Outlook calendar to help eliminate scheduling conflicts.

Users may store personal contact information in their Outlook contacts folder.

PROHIBITED USES OF STATE E-MAIL:

State e-mail systems shall not be used for the creation or distribution of any disruptive or offensive messages, including offensive (vulgar or pornographic) content or offensive comments about a person's

race, gender, age, appearance, disabilities, political beliefs, or religious beliefs and practices.

Employees

who receive any e-mail with this content from any State employee should report the matter to their supervisor immediately. Additional prohibited uses of e-mail are addressed in State standards.

In addition, the following activities are prohibited:

- ☐ **Sending or forwarding remarks and/or images considered obscene, offensive, racist, libelous, slanderous, or defamatory (as defined, where applicable, in The Code of Alabama 1975)**
- ☐ **Using an individual State e-mail account to send or forward virus or malware warnings, security advisories, terrorist alerts, or other official warning, alert, or advisory messages without prior approval of the agency IT Manager, Agency Information Security Officer, or Chief Information Security Officer (unless in the course of normal assigned duties)**
- ☐ **Sending unsolicited e-mail messages including junk mail, spam, or other advertising material to individuals who did not specifically request such material except in the execution of normal government information dissemination**
 - ☐ **Postings to newsgroups by personnel using a State e-mail address unless in the course of business duties**
- ☐ **Sending unsolicited e-mail messages including junk mail, spam, or other advertising material to individuals who did not specifically request such material except in the execution of normal government information dissemination**
 - ☐ **Postings to newsgroups by personnel using a State e-mail address unless in the course of business duties**
- ☐ **Using State e-mail for personal or commercial ventures, religious or political causes, endorsement of candidates, or supporting non-government organizations**
 - ☐ **Sending or forwarding chain letters or joke e-mail**
 - ☐ **Disguising or attempting to disguise your identity when sending e-mail**
 - ☐ **Sending e-mail messages using another person's e-mail account**
 - ☐ **Intercepting e-mail messages destined for others**
- ☐ **Unauthorized use, forging, or attempting to forge e-mail header information or messages**

State of Alabama – Policies and Standards

AUTO-FORWARDING STATE E-MAIL:

To preclude inadvertent transmission of inappropriate information onto the Internet, auto-forwarding shall not be used to send State e-mail to an Internet e-mail address.

MASS E-MAIL:

Material sent to group distribution lists must be relevant to the group being mailed and shall pertain to

State business and/or serve the interests of State employees or constituents.

Message Content/Format:

Message format may be text, HTML, or RTF and should not include attachments.

HTML or RTF format messages may contain artwork, but shall be limited to a single page.

Each message shall contain a signature block with the sender's name, departmental affiliation, office telephone number, and e-mail address.

Sender is responsible for all replies, responses, and complaints.

Message Approval:

It is the responsibility of the sender/requestor of a mass e-mail to obtain the necessary approval from the

person, group, or designated owner of the distribution list.

Authority to use the "all-employees" distribution list rests with the Governor's office.

Approval authority for agency/organization-level groups (e.g., "ISD – All Users") shall rest with the manager or management team presiding over that group.

Message shall include a line indicating the State office that approved the mass e-mail.

Message Transmission:

Mass electronic mailings shall only be transmitted in the evenings (after 5pm).

List Owner Responsibilities:

Owners of group distribution lists shall develop and monitor compliance with written operating procedures

for the use of their lists. All list owners are encouraged to consider the benefits of moderating or otherwise

controlling access to large lists. This applies whether a list has been created for one-time use or is maintained as a standing list.

INSTANT MESSAGING POLICIES

Instant Messaging (IM) is subject to many of the same threats as e-mail (known security holes, information leaks, vulnerability to malware, etc.), and IM users are frequently the target of phishing attempts. For these reasons the following policies shall apply to all IM communications.

- ☐ IM shall be used only for business communications (it is not provided for personal use).
 - ☐ IM shall not be used to communicate sensitive or confidential information.
 - ☐ IM shall be limited to text messages only; IM file transfers shall be blocked.
- ☐ IM is correspondence that creates a record that can be subpoenaed and used as evidence in litigation or regulatory investigations; therefore, IM correspondence shall be retained in accordance with applicable State data and record retention policies.
- ☐ IM content, created, stored, transmitted, or received using State resources, is the property of the State. Nothing in this policy shall be construed to waive any claim of privilege or confidentiality of IM content. Authorized State personnel may access, monitor, or disclose IM content for any business purpose or to satisfy legal obligations.

State of Alabama – Policies and Standards

REMOVABLE STORAGE DEVICE POLICIES

Removable non-volatile storage devices (USB Flash drives, PC Cards, FireWire devices, MP3 players, camcorders, digital cameras, etc.) have the same vulnerabilities as disk media (malware, data loss) but

greater capacity, and could be used to infect an information system to which they are attached with malicious code, could be used to transport sensitive data leading to potential compromise of the data, and

are frequently lost or stolen. Careful attention to the security of such devices is necessary to protect the data they may contain. For these reasons the following requirements apply to the use of

removable
storage devices.

No removable storage device shall be attached to a State information system unless approved by the IT Manager.

The IT Manager shall maintain an inventory of all approved removable storage devices and ensure controls are in place to protect the confidentiality, integrity, and availability of State data.

Removable non-volatile storage devices shall be secured, marked, transported, and sanitized as required

by State standards in the manner appropriate for the data category they contain.

Removable non-volatile storage devices shall, whenever possible, be formatted in a manner that allows

the application of Access Controls to files or data stored on the device.

Sensitive or confidential data shall not be stored on any removable non-volatile storage device unless encrypted in accordance with applicable State standards. For devices that do not support encryption of

the storage media, sensitive and confidential data shall, as promptly as possible, be transferred to a device that does support the required encryption and access controls. In the interim, the device shall be

securely stored apart from its storage media (whenever possible) and physical security must be assured.

Organizational procedures shall clearly define the handling requirements for such data and devices, and device users shall be made aware of the risks and procedures.

Virus-scan all portable storage media (diskettes, CDs, USB drives, etc.) before files residing on the media are transferred or accessed.

Maintain physical security of removable storage devices. Report immediately the loss or theft of any device containing any State data.

User awareness training shall describe the risks and threats associated with the use of removable storage devices, the handling and labeling of these devices, and a discussion of the devices that contain persistent non-removable memory.

SOFTWARE LICENSING AND USE POLICIES

Under the provisions of U.S. copyright law, illegal reproduction of software can be subject to civil and criminal penalties including fines and imprisonment. Therefore, all system users must use only properly

licensed software and must use that software in accordance with the terms and conditions of the license agreement.

State of Alabama – Policies and Standards

Information Technology Users shall NOT:

- ☐ Copy, download, nor install unlicensed software
- ☐ Install personally-owned software onto State-managed computer systems
- ☐ Install State-owned software on any non-State-owned computer systems, including home computers, unless specifically authorized in the software license agreement

Agency IT Managers shall:

- ☐ Ensure only software that is licensed to the organization is installed and used
- ☐ Ensure software is installed and used in compliance with the license agreements
- ☐ Routinely perform software audits to ensure policy compliance
- ☐ Remove any software found on State information systems for which a valid license or proof of license cannot be determined

The term “software” includes the program, media, and licenses for all operating systems, utilities, services, and productivity tools whether freeware, shareware, open source, off-the-shelf, or custom developed without regard to the system(s) on which it is installed (workstation, server, etc.).

SOCIAL MEDIA POLICIES

State agencies desiring to enhance their ability to communicate and interact with the public are turning to

social media technologies such as weblogs, wikis, Facebook®, Twitter®, etc.

As with most technologies, social media poses certain risks including but not limited to:

- ☐ Adverse impact to network bandwidth
- ☐ Reputational risk to personnel, the agency, and the State
- ☐ Potential exposure or leakage of sensitive or protected information (such as copyrighted material, intellectual property, personally identifying information, etc)
- ☐ Potential avenue for malware introduction into the organization’s IT environment

The following policies are established to address and minimize these risks and define the allowable and

prohibited uses of social media technologies in the State IT environment.

SOCIAL MEDIA USE:

Organizations may utilize commercial social networking websites (such as Facebook and Twitter) or

integrate social media capabilities (such as a wikis or weblogs) into State-hosted websites.

Information Services Division (ISD) Responsibilities:

ISD will provide security awareness training to educate users about the risks pertaining to social media

and social networking, and provide best practices for risk remediation.

Agency Management Responsibilities:

- ☐ Conduct a formal assessment of the risk resulting from agency use of social media technologies.
 - ☐ Assign appropriate personnel (Public Information Officer) to oversee the use of agency social media, evaluate and authorize agency requests for usage, and determine appropriateness of the content posted to social media sites.
- ☐ Understand that social media website contents are public records that must be retained and archived in accordance with applicable agency records disposition requirements.
- ☐ Obtain ISD approval before integrating social media capabilities on any websites hosted, developed, or administered by ISD.

State of Alabama – Policies and Standards

- Periodically review social media usage to ensure it continues to reflect the agency's communication strategy and priorities.

Agency IT or Website Administrator Responsibilities:

- Disable (if possible) any unnecessary functionality within social media websites or applications, such as instant messaging (IM) and file upload/exchange.
- Minimize or eliminating links to other websites, such as "friends", to minimize the risk of exposing a government user to a link that leads to inappropriate or unauthorized material.
- Suppress any commercial or third-party advertisements (sometimes present when using freeware versions of social media software or tools).
 - Monitor (and filter as necessary) all social media website content posted and/or viewed.
 - Prohibit/block file uploads to the maximum extent possible. Where file uploads are allowed, ensure all user-submitted files are automatically virus scanned.
- Include appropriate statements on State-hosted social media sites advising users of the public nature of the information they post.

User Responsibilities:

- Social media may not be used for personal gain, conducting private commercial transactions, or engaging in private business activities.
- Understand that postings to social media websites immediately become part of a public record.
 - Users shall not post or release proprietary, confidential, sensitive, personally identifiable information (PII), or other state government Intellectual Property on social media sites.
 - Users who connect to social media websites through State information assets, who speak officially on behalf of the state agency or the State, or who may be perceived as speaking on behalf of an agency or the State, are subject to all agency and State requirements addressing prohibited or inappropriate behavior in the workplace, including acceptable use policies, user agreements, sexual harassment policies, etc.
- Users shall not speak in social media websites or other on-line forums on behalf of an agency, unless specifically authorized by the agency head or the agency's Public Information Office.
 - Users may not speak on behalf of the State unless specifically authorized by the Governor.
- Users who are authorized to speak on behalf of the agency or State shall identify themselves by: 1) Full Name; 2) Title; 3) Agency; and 4) Contact Information, when posting or exchanging information on social media forums, and shall address issues only within the scope of their specific authorization.
 - Users who are not authorized to speak on behalf of the agency or State shall clarify that the information is being presented on their own behalf and that it does not represent the position of the State or an agency.
- **Users shall not utilize tools or techniques to spoof, masquerade, or assume any identity or credentials except for legitimate law enforcement purpose or for other legitimate State purposes as defined in agency policy.**
- **Users shall use different passwords for different accounts; do not use the same password for both a social media site and state network or e-mail accounts.**

Personal Use of Social Media Sites:

- **Employees may use personal social media for limited family or personal communications during normal business hours so long as those communications do not interfere with their work.**
- **Employees and their managers are responsible for exercising good judgment regarding personal use.**

State of Alabama – Policies and Standards

- ❑ **Users shall not use their state e-mail account or password in conjunction with a personal social media site.**

Additional Recommended Security Measures:

For added security, all users of Facebook are encouraged to enable SSL activation in their Facebook account settings.

POLICY ENFORCEMENT REPORTING:

Users should report security-related issues and policy non-compliance to their immediate supervisor, manager, or as outlined in the applicable information security policy, standard, or procedures.

NON-COMPLIANCE:

Employee conduct or behavior while using any State-managed information system must comply with ISD information security policies. Violation can result in disciplinary action up to and including termination.

Conduct or communications which violate State or Federal laws will not only be grounds for immediate termination, but may also subject the employee to criminal prosecution. Suspected violators of any laws, including copyright laws and FCC regulations, involving information services provided by the State of Alabama will be reported to the appropriate agency head and/or the Attorney General of Alabama for investigation and appropriate legal action. Some policy non-compliances may be punishable under The Code of Alabama 1975 (Section 13A-8-100 through 13A-8-103), Alabama Computer Crime Act. Such cases will be referred to the appropriate authorities.

Other policy non-compliances by users shall be handled in accordance with the applicable disciplinary guidelines established by the user's agency. ISD will determine on a case-by-case basis when policy noncompliance is sufficient grounds to deny the user access to information services.

ENFORCEMENT DIVISION

Four Charged With Underage Alcohol Sales

An undercover investigation into illegal alcohol sales to minors resulted in four arrests. ABC Agent David Taylor



conducted 25 alcohol compliance checks in Jackson County. Agent Taylor sent an underage minor operative into 25 locations in Scottsboro, Stevenson, and Bridgeport, and attempted to purchase alcohol beverages. In two of the locations, identification was not checked. The charges included selling alcoholic beverages to a minor, and furnishing alcoholic beverages to a minor. Each business faces a minimum fine

of \$750 for a first offense. Three offenses within a three-year period can result in a suspension or revocation of alcohol license.



Flag Cocktail

Ingredients:

3 ounces cranberry juice
or 3 ounces of fruit punch

3 ounces Gatorade sports
drink (blue)

3 ounces diet 7-up or 3
ounces diet Sprite

Ice cube (fill glass to top
with cubes)

Directions:

Place ice cubes in the
bottom 3rd of a tall 12
ounce clear glass. Pour
the cranberry juice or
fruit punch in to the fill
the bottom 3rd.

Place a few more ice cubes in to the middle and pour in the blue
Gatorade to fill the glass $\frac{2}{3}$ full.

Place the final 3rd of the ice cubes in the glass. Pour in the 7-up
or Sprite.

Serve and Enjoy



If you would like to have something placed in the Newsletter
please use the following contacts:

Accounting: Pam Vojnovski (pam.vojnovski@abc.alabama.gov)

Auditing: Sissy Harris (sissy.harris@abc.alabma.gov)

Enforcement: Carolyn Burdette
(carolyn.burdette@abc.alabama.gov)

Information Technology: Sylvia Temple
(sylvia.temple@abc.alabama.gov) or
Stephen Mitchell (stephen.mitchell@abc.alabama.gov)

Personnel: Nan Hahn (nan.hahn@abc.alabama.gov)

Product Management: Britney Thames
(britney.thomas@abc.alabama.gov)

Warehouse: Betty Flowers (betty.flowers@abc.alabama.gov)

Stores Central Office and Administrator's Office:

Debra Moore (debra.moore@abc.alabama.gov)
or Jennifer Holton (jennifer.holton@abc.alabama.gov)

Store Personnel should contact their District Supervisor!

**If you have any questions please do not hesitate to
contact me either by phone or email.**

Debra S. Moore

334-260-5425